

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

FILED

SEP 02 2016

Clerk, U. S. District Court
Eastern District of Tennessee
At Greeneville

IN THE MATTER OF THE SEARCH OF A)
HEWLETT PACKARD LAPTOP COMPUTER,)
SERIAL NO. 0019-205-614-545, A SEAGATE)
EXTERNAL HARD DRIVE, SERIAL NO.)
NA47J2WQ, TWO (2) PNY 128GB THUMB)
DRIVES, ONE (1) SANDISK 8GB THUMB)
DRIVE, AND ONE (1) SANDISK 2GB THUMB)
DRIVE)

No. 2:16-MJ- 166
JUDGE CORKER

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Travis Carrier, being duly sworn, hereby depose and state:

1. That I have been a duly authorized Special Agent with United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) since 2008. Prior to that, I was a Federal Agent with the United States National Nuclear Security Service (NNSA) since 2005 and a police officer for the state of Tennessee from 1997 to 2004. I am currently assigned to the Tri Cities, Post of Duty (POD). Included in my responsibilities are overseeing and conducting federal and international investigations relating to crimes involving the sexual exploitation of children. I have participated in and conducted investigations involving the sexual exploitation of children in violation of Title 18, United States Code Section § 2252A, which relates to the knowing transportation, shipment, receipt, possession, distribution, and reproduction of child pornography.

2. I am investigating the activities of a person, Steven Gregg, who is believed to have received a video of child pornography in 2013, and has admitted to viewing child pornography from the Internet on his personal laptop. The transportation, reception and possession of child pornography, is a violation of Title 18, United States Code, § 2252A. As will be shown below,

there is probable cause to believe that fruits, evidence and instrumentalities of the unlawful transportation, receipt, distribution, and possession of child pornography are located on Steven Gregg's laptop, currently in the possession of Homeland Security Investigations. All the information contained in this affidavit is based on my investigation and personal knowledge, information provided to me by other law enforcement officials, and information from records checks conducted by law enforcement officials. This affidavit is being submitted for the limited purpose of securing a search warrant, and therefore I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 2252A, are presently located on the devices described further in Attachment A.

STATUTORY AUTHORITY

3. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors and child pornography.

a. 18 U.S.C. § 2252A (a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A (a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. § 2252A (a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.

d. 18 U.S.C. § 2252A (a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

e. 18 U.S.C. § 2252A (a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

TERMS APPLICABLE TO THIS AFFIDAVIT

4. INTERNET SERVICE PROVIDER: A company that provides its customers with access to the Internet, usually over telephone lines or cable connections. Typically, the customer pays a monthly fee, and the Internet Service Provider ("ISP") supplies software that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

5. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

6. INTERNET PROTOCOL ADDRESS ("IP address"): The unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in four

blocks of numbers, as in 123.456.789.001, just for example. Each number can only be used by one computer or machine over the Internet at a time. Other numbers such as "mac" addresses or port numbers may further distinguish devices or machines sharing a connection, but the IP address identifies the point at which a computer or machine is connected to the internet, normally via a modem.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Your affiant knows all of the below-described information as the result of his training and experience in the investigation of computer-related crime and by conferring with other law enforcement personnel who investigate computer-related crime.

8. Your affiant knows that computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. They also have revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies).

9. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

10. The advancement in technology of computers, smartphones and tablets has added to the methods used by child pornography collectors to interact with and sexually exploit children.

Each of the above serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

11. Child pornographers can now produce both still and moving images directly from a common video camera, small action style cameras such as a GoPro, smartphones, laptop computers equipped with web cameras, and tablets. In the past, a camera could be attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer, external hard drive, media card (SD, Compact Flash, micro SD, memory stick), smart phone, tablet, iPod or iPad. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is inexpensive and technically easy to produce, store, and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as had been the case in the past. Your affiant has been involved in recent investigations where digital cameras, smart phones, tablets and webcams were used to produce child pornography and store said child pornography either on the device, personal computer or removable media of the subject.

12. New technology now allows child pornographers to use even smaller digital devices like smartphones and tablets that have digital cameras and video recording capability built directly into the devices. These devices are equipped with their own processors and memory that allow the devices to actually perform as small mini computers. With the use of free and publicly available apps, a child pornographer has the ability to produce child pornography, receive and

distribute it in a matter of just a few seconds and maintain relative anonymity using free open wireless access points.

13. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer also has changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone and/or cable lines. By connecting to a host computer, electronic contact can be made with literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Bellsouth, AT&T and America Online, which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. Today many ISPs, such as Comcast Communications and Charter Communications, offer high-speed broadband Internet service. Broadband is often called high-speed Internet because it usually has a high rate of data transmission much higher than the dial-up or DSL structure of the past. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms" and/or instant messaging.

14. These communication structures are ideal for individuals who possess, receive and distribute child pornography. They provide open and anonymous communication, allowing users to locate other persons who share their interest in child pornography, while maintaining their anonymity. Once contact has been established, it is then possible to send text messages, graphic images, and high-resolution video to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use

standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornographers.

15. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via electronic mail to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, P2P services and easy access to the Internet, the computer is a preferred method of receipt and distribution of child pornographic materials.

16. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly consisting of hard drives) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of one terabyte are not uncommon.

17. Homeland Security Investigations Computer Forensic Agents routinely examine computer hard drives of five-hundred (500) gigabytes and more in child pornography cases. These drives can store tens of thousands of images and video at very high resolution and quality. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, save the image, and store it at another location. Once this is done, there is no readily

apparent evidence at the scene of the crime. Only with careful examination of electronic storage devices is it possible to recreate the evidence trail.

18. Based on your affiant's knowledge, training and experience and training and experience of other officers, your affiant knows that child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads so the images can be maintained in a manner that is both mobile and easily accessible to the collector. It is not uncommon for the child pornographer to print pictures of child pornography and to keep them in a safe and secure location for easy viewing. Thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, computer game consoles (Sony PlayStation, Xbox), tablets, iPod's or iPads, containing child pornography and printed pictures of child pornography are not only kept near the computer, but also in hidden areas known to the child pornographer, to keep other individuals from discovering the illegal material.

19. Your affiant states that computer technology can be mobile in the form of laptop computers, removable thumb drives, removable hard drives, media cards (SD, Compact Flash, micro SD, memory stick), computer game consoles (Sony PlayStation, Microsoft Xbox), smart phones, iPad's, iPod's, tablets, or accessible via remote or wireless means. Therefore, evidence, contraband, instrumentalities, or fruits of crime can be located virtually anywhere within the residence or vehicle of a child pornographer. Additionally, child pornography can remain on devices indefinitely unless the user takes active steps to delete or overwrite the digital files of child pornography. However, computer forensic agents have revealed that even if the above

methodology is utilized examiners are able to locate and recover evidence about the criminal activity including but not limited to the files child pornography, software used to locate and download child pornography, and log files identifying specific child pornography files that have been downloaded to the computer system of the suspect.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

20. Based on my training and experience, your affiant knows that the search of computers and retrieval of data from computer systems and related media, often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following.

21. Computer storage devices like thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, computer gaming consoles (Sony PlayStation, Xbox), tablets, iPods or iPads can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

22. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and

applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting Scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from a destructive code imbedded in the system such as a "booby trap," a controlled environment is essential to its complete and accurate analysis.

23. Based upon your affiants training and experience and consultation with experts in computer searches, data retrieval from computers, and related media, as well as consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all computer system input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following: The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst

determines that the I/O devices, software, documentation, and/or data security devices are not necessary to retrieve and preserve the data after inspection, the government will return the material within a reasonable time.

24. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any application software, which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

25. Based on your affiant's training and experience in computer searches and data retrieval from computers while in a laboratory setting, your affiant is aware that such searches can be complex and time consuming.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

26. The property to be searched is a Hewlett Packard Laptop Computer, Serial No. 0019-205-614-545, hereinafter "the Laptop." a Seagate external hard drive, Serial No. NA47J2WQ, (2) PNY 128 GB thumb drives, (1) SanDisk 8 GB thumb drive and (1) SanDisk 2 GB thumb drive. The devices are currently located at 324 Prosperity Drive, Knoxville, Tennessee in the custody of Homeland Security Investigations. I obtained the laptop, hard drive, and thumb drives from Steven GREGG, at 2028 Queensbury Court, Kingsport, Tennessee, on August 11, 2016, where the suspect of this investigation, Steven GREGG, resides and consented to the search of the laptop computer. The property to be searched is further described in Attachment A.

27. The applied-for warrant would authorize the forensic examination of the laptop, hard drive, and thumb drives for the purpose of identifying electronically stored information and data particularly described in Attachment B, which is incorporated by reference herein.

PROBABLE CAUSE

28. Homeland Security Investigations, Knoxville, Tennessee received a lead from the Child Exploitation Investigations Unit to investigate the user of luvbigpups@aol.com for the suspected purchase of child pornography. Steven GREGG of Kingsport, Tennessee, was identified as having sent \$500.00 via Western Union to an individual who is associated with a child pornography website.

29. A summons submitted to AOL for subscriber information relating to luvbigpups@aol.com revealed the account belonged to Steven Gregg of Kingsport, Tennessee.

30. In October of 2013, the Child Exploitation Investigations Unit (CEIU) began to review cyber tip line reports from the National Center for Missing and Exploited Children (NCMEC) that documented what appeared to be a website offering child pornography for sale. CEIU obtained the contents of several email accounts associated with the website in question, one of them belonging to someone identified only as ANTONIN.

31. CEIU discovered luvbigpups@aol.com exchanged two emails with ANTONIN, with no content, but having the subject line "30daysvideomemberhiop-500". On December 24, 2013, luvbigpups@aol.com sent an email to ANTONIN, providing him with a Western Union MTCN 4868187017 (transaction number) for the transfer of \$500.00, which was sent from Steven GREGG of Kingsport.

32. CEIU issued a summons to Western Union to identify any transactions relating to Kristina Smirnova, one of the names used by the aforementioned website to receive payments. Western Union provided the requested information, which identified Steven GREGG sending a payment to Kristina Smirnova on December 24, 2013. Additionally, Western Union provided the following information as to the transaction:

- U.S. Dollars sent: \$500.00
- MTCN transaction no: 4868187017 (same as the transaction number indicated in the email from luvbigpups@aol.com to ANTONIN)
- Sender's phone: 423-276-8460
- Send Date: 12/24/2013
- Send Time: 09:54:00
- Senders credit card: 415522xxxxxx0224
- Sender's IP number: 71.88.206.171
- Sender's address: 2028 Queensbury Court, Kingsport, Tennessee, 37660.

33. On October 23, 2014, Homeland Security Investigations, Special Agent (SA) Michelle Evans received the aforementioned lead from CEIU. On October 28, 2014, Homeland Security Investigations, Special Agent (SA) Michelle Evans opened the Knoxville investigation and issued a summons to AOL for subscriber and account information relating to luvbigpups@aol.com. AOL provided the following information:

Account Screennames:

- Hongkonghing (deleted)
- Kunminggirls58

- Luvbigpups
- Userme154 (deleted)
- Vee8fusion (deleted)

Account Information:

- Billing Method: VISA
- CC Name: Steven GREGG
- Card Number: 415522xxxxxx1602
- Expiration Date: 11/14.

34. On November 21, 2014, Homeland Security Investigations, SA Michele Evans requested CEIU to send a covert email to luvbigpups@aol.com. On November 24, 2014, SA Evans received confirmation from Homeland Security Investigations, SA Kret Lukasz, that the requested email was sent to luvbigpups@aol.com. To date no reply from luvbigpups@aol.com has been received.

35. On March 16, 2015, Homeland Security Investigations, SA Michele Evans went to 2028 Queensbury Court, Kingsport, Tennessee, the residence of Steven Gregg in an attempt to interview Steven Gregg regarding the historical emails Steven Gregg sent to ANTONIN. No one was at the residence.

36. In May 2016, SA Michelle Evans requested your affiant to conduct a knock and talk at 2028 Queensbury Court, Kingsport, Tennessee, the residence of Steven Gregg and interview Steven Gregg.

37. On August 11, 2016, your affiant, Homeland Security Investigations, SA Trevor Christensen, Sullivan County Sheriff's Detective Matt Price and Kingsport Police Department

Detective Martin Taylor, Detective Price went to Steven GREGG's residence at 2028 Queensbury Court, Kingsport, Tennessee to speak with Steven Gregg. Detectives Price and Taylor are Computer Forensic Agents (CFA).

38. Contact was made with an Asian female claiming to be Steven Gregg's wife. She advised Steven was at work and would be home in approximately 40 minutes. Contact was made with Steven GREGG as he pulled into the drive way and walked to his mailbox.

39. Your affiant made contact with Steven Gregg. Your affiant identified himself and asked Steven GREGG if he would mind speaking to him. Steven GREGG agreed and your affiant asked Steven Gregg where he preferred to speak and he replied "here" (his driveway) would be fine. Your affiant and Steven GREGG moved over to your affiant's car where the shade was more prevalent. At this time SA Christensen and Detectives Taylor and Price introduced themselves to Steven Gregg.

40. Your affiant explained the nature of the visit and advised Steven Gregg he was not under arrest. Your affiant provided Steven GREGG with the historical details surrounding the aforementioned emails being sent to ANTONIN from his email address: luvbigpups@aol.com, and the sending of \$500.00 through Western Union to Kristina Smirnova on December 24, 2013.

41. Steven Gregg advised his email address was luvbigpups@aol.com, but never that he sent money to that person and did not know ANTONIN. Steven GREGG also stated he did not look at child pornography. Your affiant asked Steven GREGG if he would allow his computer to be imaged. Your affiant at that time had Detective Matt Price explain the process of imaging.

42. Steven GREGG consented to the imaging of his computer. At this time Steven GREGG was provided a consent to search form and was asked to review the form. Steven Gregg looked the form over and your affiant read the consent form to him and asked him if he had any

questions. Steven GREGG advised he understood and had no questions. Steven GREGG signed the consent to search form. Steven Gregg asked how long the imaging process took and Detective Price advised it varied from computer to computer, but could possibly take a long time to complete.

43. At this time Steven Gregg walked Officers into his residence, 2028 Queensbury Court, Kingsport, TN. Once inside the residence, Steven GREGG escorted Officers to a back bedroom, being used as an office, where a laptop was in plain view on a desk. Steven GREGG advised the laptop was the only computer he owned.

44. Detective Price, utilizing forensic software, began imaging the laptop (a gray HP, G7, serial number: 0019-205-614-545).

45. Your affiant, again, advised Steven Gregg he was not under arrest and to let him know if he (Steven GREGG) had to leave for anything. Steven GREGG advised he did not need to go anywhere. Steven GREGG repeatedly told Officers he did not know anything about child pornography and nothing of that nature should be on his computer.

46. Detective Matt Price advised your affiant he located files indicative of child pornography on Steven GREGG's laptop. The following file names were found during the imaging process:

- G:\Vids\Gracel Series_Melissa_Set13v-pthc 2011_xvid.avi
- [PTHC 2012] 12 yo Bucarest Girl Bates And let Dog Licks Her Pink Pussy! Very GOOD!
[11 yo, loli, webcam, preteen, pedo, bibcam,kids,cbaby,zoo,beastiality]_01.mpg
- V.loli.png
- Babyj_Super_Hot_5yo.3gp

47. The above terms are indicative of child pornography; PTHC, stands for Preteen Hard Core, Pedo stands for pedophile, and loli is a key word that is indicative of child pornography searches on the internet.

48. At this time, your affiant advised Steven GREGG he needed to ask him some questions related to the aforesaid mentioned file names discovered on his computer. Your affiant advised Steven GREGG that, before he asked him any further questions, his rights would be read to him. Your affiant read Steven GREGG his rights, handed the rights form to Steven GREGG and asked him to read the rights form as well. After Steven Gregg read the rights form, your affiant asked Steven Gregg if he understood. Steven GREGG advised he understood and waived his rights, agreeing to speak to your affiant and SA Trevor Christensen.

At this time, your affiant and SA Trevor Christensen interviewed Steven GREGG.

Steven GREGG made the following comments:

- I did send \$500.00 for videos pertaining to your previous questions, but can't remember to whom. I remember the videos to be of teen girls.
- This was the only video I've ever ordered. I never received the video after sending the money.
- I can't recall if it was ANTONIN or the Russian name you mentioned that I ordered the video from. It has been a long time.
- I used the laptop for which I provided consent to search today, when I viewed child porn approximately (3) years ago.
- When asked for his definition of child pornography, Steven GREGG replied: sex with underage kids and little kids having sex with men.
- My current opinion on child pornography is that it is wrong.

- I looked at child pornography out of curiosity. It has been almost (3) years ago.
- I received pop ups on my laptop that were child pornography links and I clicked on those links out of curiosity. I do not know who I received the links or pop ups from.
- When asked what age preferences he had when viewing the child pornography, Steven GREGG responded little boys and little girls.
- When asked what age preferences he had when viewing child pornography, Steven GREGG did not state an age, but presented the hand gesture as if he was measuring using the ground as a start point, measuring approximately 2ft to 4ft tall in height. Steven GREGG advised he does not have kids and is not very good at judging ages.
- I only looked at the said links for a period of two to three weeks, if that.
- I looked at child pornography links and deleted them after viewing.
- There is currently no child pornography on my computer now.
- No one is sending me child pornography links to me.
- When I viewed the child pornography, three years ago, my laptop was not password protected.
- I am the only person who has permission to use my laptop.
- I may have let a friends use my laptop, but cannot remember who or when.
- Charter was my service provider when I looked at child pornography and it is my internet provider currently.
- My laptop is not password protected, but I believe my Wi-Fi is password protected. (SA Trevor Christensen pulled up Steven GREGG's Wi-Fi (NetGear 123) and it showed to be password protected.)

- Steven GREGG stated he never used external hard drives or media to store child pornography. (Detective Matt Price determined several media devices thumb-drives and external hard drives to have been plugged into Steven GREGG's laptop. Four thumb-drives were beside the laptop.)

49. Detective Matt Price determined through the imaging process of Steven GREGG's laptop, that various external memory devices had been used on Steven GREGG's laptop: one Seagate external hard drive, two (2) PNY thumb drives, and two (2) SanDisk Cruzer thumb drives, all of which Steven GREGG showed Detective Price. Other devices, discovered to have been previously attached to Steven Gregg's laptop were: a Cannon Power Shot SD 1400 IS and an Apple mobile device USB driver (iPhone 4) were not seen in proximity to the laptop, and Steven GREGG advised he could not remember having another external hard drive. The imaging process showed the Cannon Power Shot SD 1400 IS was last used on Steven Gregg's laptop on 06/12/2016, and the last use of the Apple mobile device USB driver (iPhone 4) on Steven Gregg's laptop was 07/06/2016.

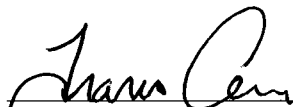
50. Prior to beginning the analysis of Steven Gregg's laptop, Detectives Martin Taylor and Matt Price conducted a security sweep for officer safety in the bedroom where Steven Gregg's laptop was located. Detective Taylor advised your affiant he observed stacks of ammunition and weapon boxes clearly visible in the closet. Detective Taylor also advised he observed several buttstocks of what appeared to be shotguns stacked in the same closet, partially covered with a blanket. Detectives Taylor and Price advised your affiant that a large sum of U.S. currency was observed in a plastic bag sitting on a table in plain view in the same bedroom. Detectives Taylor and Price advised that the currency was in a large stack of \$100.00 dollar bills inside a clear

plastic bag. SA Carrier removed a large caliber rifle that was in plain view sitting on a table in the same bedroom to another location for officer safety.

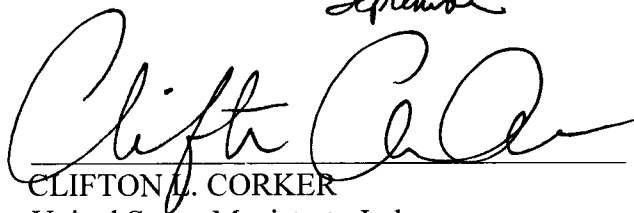
CONCLUSION

51. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe the laptop computer, hard-drive, and four thumb drives, seized on August 11, 2016, by Homeland Security Investigations from 2028 Queensbury Court, Kingsport, TN, belonging to Steven GREGG, described further in Attachment A, contain evidence of violations of 18 U.S.C. § 2252A.

52. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the items described in Attachment A.


Travis Carrier
Homeland Security Investigations

SUBSCRIBED and SWORN
Before me this 2nd of ~~August~~ 2016.


CLIFTON L. CORKER
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a Hewlett Packard Laptop Computer, Serial No. 0019-205-614-545, a Seagate external hard drive, Serial No. NA47J2WQ, two (2) PNY 128 GB thumb drives, one (1) SanDisk 8 GB thumb drive and one (1) SanDisk 2 GB thumb drive. A photograph of the items is below.



ATTACHMENT B

Information to be Seized

1. Instrumentalities of the violations contained within the continuation for the search warrant for Hewlett Packard Laptop Computer, Serial No. 0019-205-614-545, a Seagate external hard drive, Serial No. NA47J2WQ, two (2) PNY 128 GB thumb drives, one (1) SanDisk 8 GB thumb drive and one (1) SanDisk 2 GB thumb drive, hereafter referred to as COMPUTER:
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - e. evidence of the times the COMPUTER was used;
 - f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - g. records of or information about Internet Protocol addresses used by the COMPUTER;
 - h. records of or information about the COMPUTER’s Internet activity: firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search

terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

i. contextual information necessary to understand the evidence described in this attachment.